810-RD-002-001

EOSDIS Core System Project

Unclassified Automated Information System Security Plan for the ECS Development Facility

October 1995

Hughes Information Technology Corp.
Upper Marlboro, Maryland

Unclassified Automated Information System Security Plan for the ECS Development Facility

October 1995

Prepared Under Contract NAS5-60000

APPROVED BY

R.E. Clinard /s/	11/1/95
R.E. Clinard, ECS CCB Chairman EOSDIS Core System Project	Date

Hughes Information Technology Corp.
Upper Marlboro, Maryland

This page intentionally left blank.

Preface

This document has been prepared in conformance with the NASA Federal Acquisition Regulation Subpart 18-52.204-77 under agreement with the NASA Goddard Space Flight Center contracting office for the ESDIS Program. This is a new release which incorporates revisions to the July 1993 document (101-001-CO2-001) submitted previously for review.

This document is under ECS Contractor Configuration Control. Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Information Technology Corp.
1616 McCormick Dr.
Upper Marlboro, MD 20774-5372

This page intentionally left blank.

Abstract

The purpose of this document is to present general guidance on Automated Information System (AIS) management philosophies, policies, and requirements at the ECS Development Facility (EDF). Specifically, this document discusses the EDF organization, physical security, personnel security, information security, AIS security, security issues requiring coordination with NASA, and Hughes internal policies for security.

The AIS security management processes covered by this document exemplify our efforts to assure that scientific missions and business functions are carried out in an accurate, safe, accountable, and efficient manner. This document has been prepared in conformance with the NASA Federal Acquisition Regulation Subpart 18-52.204-77. This document addresses the internal security at the EDF in Upper Marlboro, Maryland. The plan addresses

a. the information security program and how administrative systems (such as accounting, property, Performance Measurement System) are protected;

b. equipment at the facility used for program management and development (such as system networks and computers);

c. software and data assets;

d. and Government property and equipment located at the facility.

This document does not address the ECS product as it will be deployed; the EDF is only the development and support environment.

Keywords: security, NHB 2410.9A, risk, threat, vulnerability, criticality, sensitivity analysis, need-to-know, access control, privacy data, security incidents, individual accountability, system stability, software protection, disaster recovery, copyright

This page intentionally left blank.

Contents

Preface

1. Introduction

2. EDF Organization

3. Physical Security

4. Personnel Security

5. Information Security

6. AIS Security

7. Security Issues Requiring Coordination with NASA

8. Hughes Internal Policies

Figures

Tables

Appendix A – Badging Policy

Appendix B – Employee Rules and Regulations

Abbreviations and Acronyms

1. Introduction

1.1 Scope

The Automated Information System (AIS) security management processes covered by this document exemplify our efforts to assure that scientific missions and business functions are carried out in an accurate, safe, accountable, and efficient manner. This document has been prepared in conformance with the NASA Federal Acquisition Regulation Subpart 18-52.204-77. This document addresses the internal security at the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Development Facility (EDF) in Upper Marlboro, Maryland. The plan addresses

a. the information security program and how administrative systems (such as accounting, property, Performance Measurement System) are protected;

b. equipment at the facility used for program management and development (such as system networks and computers);

c. software and data assets;

d. and Government property and equipment located at the facility.

This document does not address the ECS product as it will be deployed; the EDF is only the development and support environment.

1.2 Purpose

The purpose of this document is to present general guidance on AIS management philosophies, policies, and requirements at the EDF. Specifically, this document discusses the EDF organization, physical security, personnel security, information security, AIS security, security issues requiring coordination with NASA, and Hughes internal policies for security.

1.3 Period Covered

This document covers the period from the start-up operations at the EDF and will be superseded by any revisions to referenced plans, procedures or policies cited in the ECS Security Plan.

1.4 Relationship to Other Plans

This Unclassified Automated Information System Security Plan for the EDF document is considered to be an adjunct to the formal Contract Deliverable Requirements List Item 034 ECS Security Plan (Data Item Description (DID) 214/SE1) which addresses the product EOSDIS Core System (ECS) deployment. There are several other related plans such as the Security Analysis Report (DID 215/SE3), Hazard Analyses (DID 513PA2), Security-Sensitive Items List (DID 514/PA2), Failure Modes and Effect Analyses and Critical Items List (DID 517/PA2), and Software Critical Items List (DID 520/PA2).

The Unclassified Automated Information System Security Plan for the EDF document has spawned two contingency plans that are currently in use at the EDF. The ECS Development Facility (EDF) Disaster Recovery Plan (811-RD-001-001) describes the Disaster Recovery procedures that are currently in place at the Upper Marlboro, MD EDF. In the event of an emergency or disaster affecting the EDF, this plan will be followed to provide for the safety and the protection of company and Government computer resources and data assets. A complementary document, Emergency Preparedness Plan (812-RD-001-001), addresses issues related to safeguarding personnel, visitors, and non-data processing assets.

1.5 Applicable Documents

The following documents are applicable only to the extent stated herein. The latest revision in effect at the time of use will be considered. In the event of conflict between these documents and the ECS contract, the ECS contract will take precedence.

- IEEE 1003.6 POSIX Security, Draft 12c, July 1992
- NASA Goddard Space Flight Center Security Manual, GHB 1600.1A
- OMB Circular A-130, Management of Federal Information Resources
- OMB Circular No. A-127, Financial Management Systems
- Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28-STD)
- National Computer System Laboratory (NCSL) Bulletin, Guidance to Federal Agencies on the Use of Trusted Systems Technology, July 1990
- Government Network Management Profile (GNMP), Version 1.0, December 14, 1992
- NMI 2410.7A, Assuring the Security and Integrity of NASA Automated Information Resources, July 8, 1988
- NMI 8610.22, National Resource Protection (NRP) Program, December 5, 1989
- NHB 2410.9, Automated Information Security, Volume I, September 1990
- NHB 2410.1D (as amended) Chapter 3, Privacy and Security for Automated Information Processing Resources, April 1985
- 1989 Computer Security and Privacy Plans (CSPP) Review Project: A First-Year Federal Response to The Computer Security Act of 1987 (Final Report)
- NASA Security Handbook NHB 1620.3C, February 1993 Edition
- ECS Development Facility (EDF) Disaster Recovery Plan, document #811-RD-001-001
- Emergency Preparedness Plan, document #812-RD-001-001)
- EDF Network Configuration, document # 811-TD-006-001, 3/7/95
- EDF Routing Topology, document # 811-TD-005-003, 3/7/95
- EDF Computer Floor Layout, document # 811-TD-007-001, 3/7/95

2. EDF Organization

2.1 Responsibilities

The Maintenance and Operations (M&O) Manager has broad scoping responsibilities for technical management of the resources to direct, control, and perform maintenance and operations for the overall ECS including the segment elements at each of the ECS sites and in support of each of the hardware deliveries and software releases. M&O management includes M&O control, property management, configuration management, security, operational readiness and performance assurance and general support.

The EDF Manager reports to the M&O Manager and has overall responsibility for the operation of the EDF. As such, he is responsible for both operations, maintenance and control of all hardware and software within the EDF environment and the enforcement of security. The EDF manager is responsible for ensuring that the security mechanisms are designed into the EDF system and that the proper procedures and documentation are in place.

Within the EDF organization, the System Manager is responsible to the EDF Manager for directing the maintenance and operations personnel in the performance of their assigned duties. Various functional organizations responsible to the EDF Manager perform security-related duties as shall be explained in subsequent text. The EDF organization is depicted in Figure 2-1.

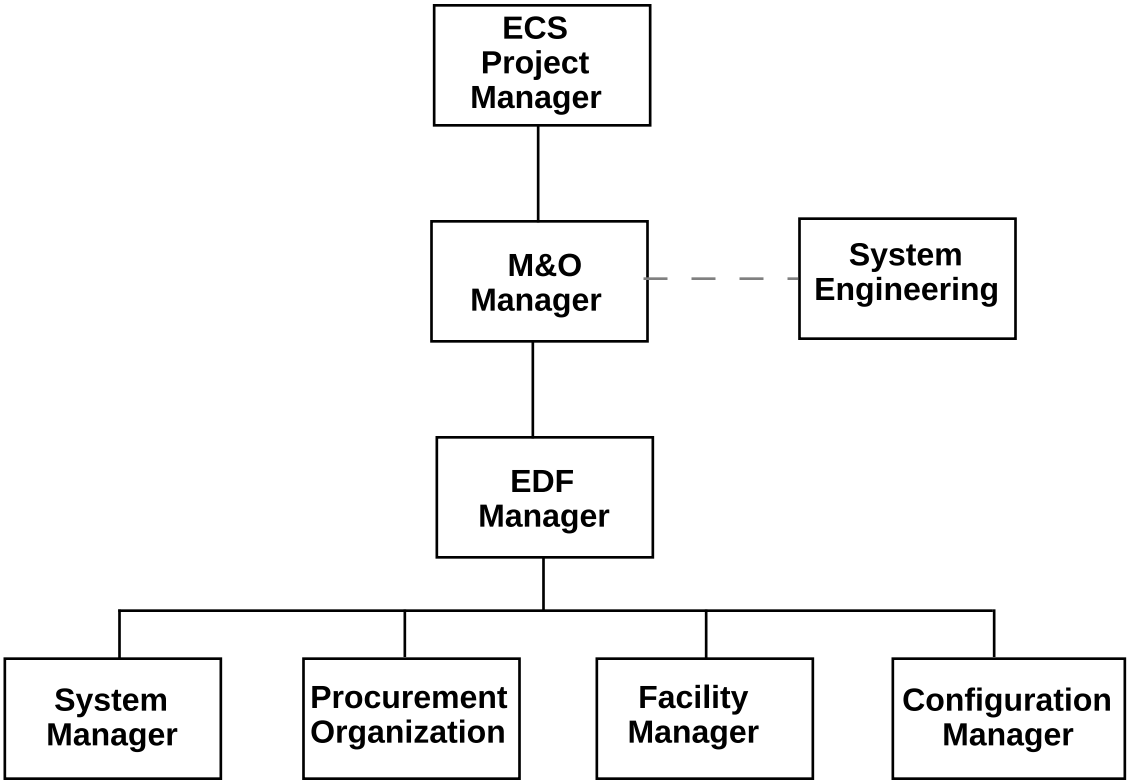

Figure 2-1. EDF Organization Chart

2.1.1 Project Manager

The ECS Project Manager provides overall guidance and policy to the M&O organization, which includes the EDF. These policies are then reflected in applicable command media and program instructions.

2.1.2 System Engineering

The System Engineering organization provides design requirements for the EDF in terms of the hardware and software suites required to support ongoing development as well as ancillary functions. These requirements are translated into two categories of purchase requests:

a. capital and expense requests which are funded by Hughes Applied Information Systems Inc., (HAIS), and

b. program-funded requests which are processed by the Procurement Organization.

2.1.3 Facility Management

The Facility Manager reports to the EDF manager and is tasked as the Computer Security Officer (CSO) for the EDF physical plant with the responsibility of providing overall physical security of HAIS facilities, including access control to sensitive areas such as the computer room. The Facility Manager shall perform periodic audits of the physical property control system, issue Property Management Reports, and make any needed maintenance adjustments in accordance with the Uniform Property System, HAIS Practice 9-3-13. The Facility Manager is also responsible for badging all ECS personnel as well as visitors and customer personnel. Badging is further discussed in Paragraph 4.4 below.

2.1.4 System Management

The EDF computing system is managed by the System Manager who performs system operation in the entire EDF and maintains Hughes capital equipment (office automation and administration) with support from vendor maintenance. The System Manager will also act as the Computer Security Officer (CSO) for the Automated Information System (AIS) to ensure compliance to computer network security procedures by System Users. The Procurement Organization will perform installation and maintenance of ECS Contractor Furnished Equipment, i.e., equipment purchased under contract funding, which is operated by the System Manager. The System Manager will perform installation and maintenance of Contractor-owned Equipment Accountability for the evolving EDF configuration baselines will be maintained by the Configuration Manager.

The System Manager is responsible for protection and detection of loss of equipment. Periodic audits will be performed to verify network parameters (e.g., user accounts, access controls, passwords, etc.), software (e.g., applications licensing, revisions, backup, etc.), and equipment (property control).

2.1.5 System Users

System users are responsible for adhering to all program security policies and procedures, to include physical security as well as electronic security, e.g., password confidentiality. Users failing to comply with program security requirements will be sanctioned in accordance with program management policy.

2.2 AIS Plans and Procedures Schedule

The schedule contains related AIS security documentation schedules and M&O reviews against a backdrop of ECS Project milestones for early evolution and deployment of the ECS product which is supported by the ECS Development Facility (EDF). Figure 2-2 shows the major annualized reviews of EDF AIS Backup Test, Software Audits, Network Certifications/Audits, Equipment Audits, Facility Audits and AIS Security Contingency Plans.

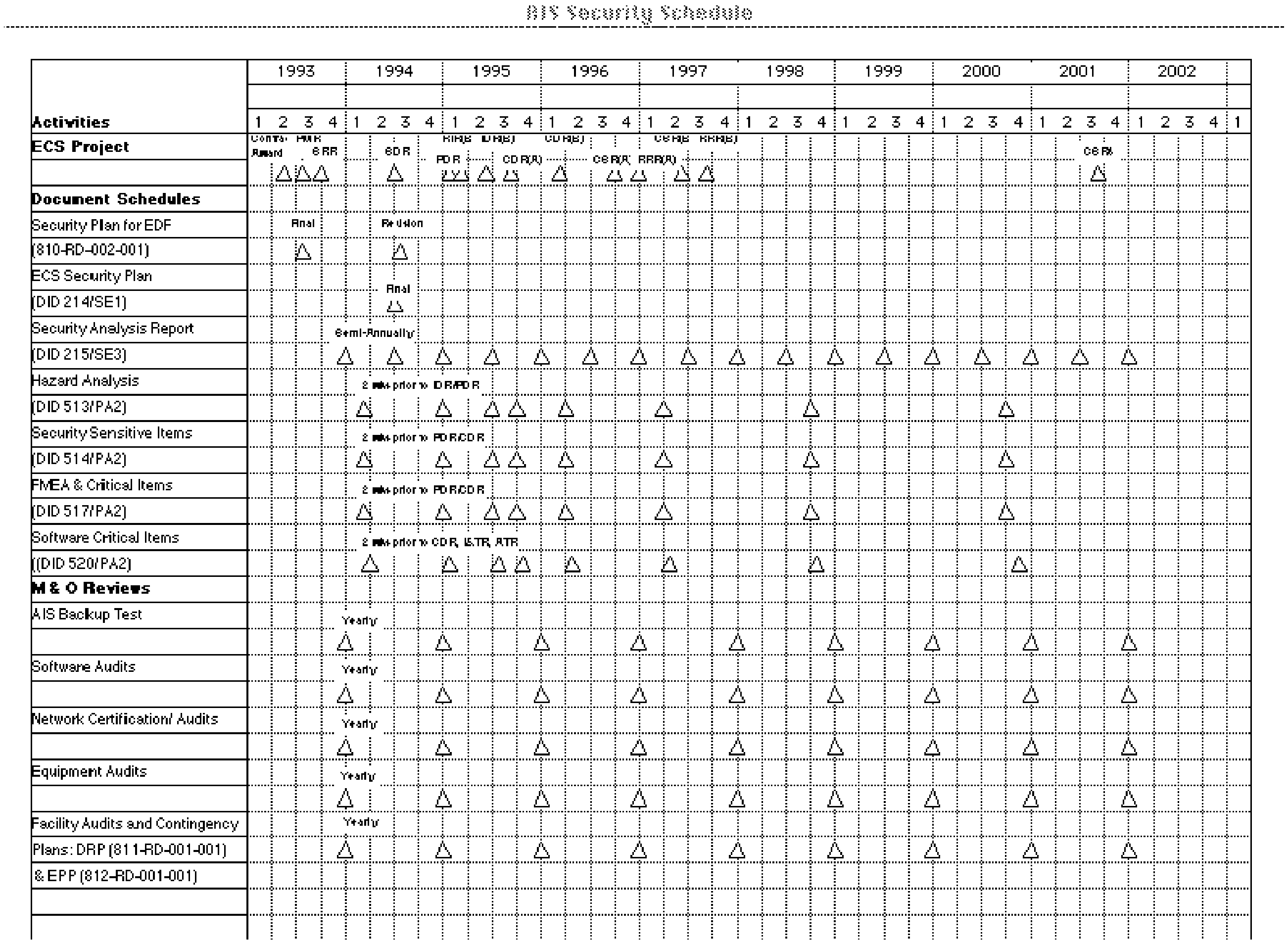

Figure 2-2. AIS Security Schedule for the EDF

2.3 Security Incidents

We will implement a threat and incident reporting system in accordance with NHB 2410.9 and NHB 1620.3C. The purpose is to keep project management informed on a timely basis of serious security-related incidents or threats that may affect the performance of the ECS contract or compromise the security of personnel and property in our care. Reports shall be prepared and channeled to ECS management by security personnel as an aid to proper response for mitigation of losses and loss prevention. In the event of serious threat information, this report will be secondary to the notification of appropriate law enforcement or response agencies. The NASA COTR would be notified formally by the format of Appendix Q in NHB 1620.3C.

The Computer Security Incident Response reporting and follow-up actions shall be implemented by a combination of standard corporate procedures (11-1-12, Electronic Data Processing Security Program and 18-2-2, Protection of Information Systems) and NHB 2410.9, Section 803, item (e). Our approach features a combination of notification, deterrent measures, measured response, and trend analysis to prevent unauthorized use, sabotage, or loss of information system assets.

2.4 Security Audits, Evaluation, Review, and Training

The Computer Security Officer will perform regular maintenance checks of the network and individual workstations to ensure the proper software configuration, use of virus checking utilities, use of authorized/licensed applications software, proper backup of servers, etc. It is the responsibility of individual workstation users to backup personal files to the network server. Section 4.2 discusses training of employees, subcontractors, and visitors for security awareness. The configuration manager will keep records of EDF baseline configurations to facilitate audit and reviews.

Maintenance and Operations will perform periodic evaluations and audits of the facility and operations. The schedule of these reviews has been addressed in Section 2.2.

This page intentionally left blank.

3. Physical Security

3.1 General

Physical Security describes those measures taken to protect all information, data, personnel, equipment, and property from damage, loss, theft, sabotage and related acts that include disasters, fire, and injury to personnel. Physical security is the chief responsibility of the Facility Manager at the EDF under the auspices of the ECS Project Manager.

3.2 EDF Physical Security

3.2.1 General

EDF physical security consists of a combination of access controls; log-in accountability for after-hours and visitor access; detection systems (motion detectors, 24 hour remotely monitored cameras, fire and smoke alarms, door alarms); 11 hour staggered shifts of receptionists; employee badging system; property identification system; sprinkler system, backup power (UPS and Generator); internal communications system for voice and data; and security locks for files, access doors, and elevators. The Plant Protection Office is located at Room 1120. Detailed procedures for physical security are listed in Hughes Standard 11-1-3.1, Revised.

3.2.2 EDF Access/Controls

Access controls utilized at the EDF consist of the following:

After-Hours Log-in— Sign-in logs will be completed by employees and visitors who enter the EDF before 5:30 AM or after 10:00 PM on normal working days and anytime on weekends and holidays. Employees who have entered the facility during normal working hours and elect to remain after 8:00 PM must indicate their presence by signing the after-hours log by 10:00 PM.

Control of Receiving Dock Entrance— A telephone allows call-in to receiving clerk. M&O employees assigned to the receiving areas will unlock/lock entrance to receive or dispatch an item. The outer doors will remain locked at all other times.

Personnel Access— Badges are provided to visitors and personnel as detailed in Appendix A under the governance of the Plant Protection Office. Lost badges must be reported within one day of when they are discovered missing. Badges reported lost will be removed from the badge access control system and upon their recovery must be returned to the Plant Protection Office. Fees will be assessed for lost badges.

Computing Facility— Limited access to the central computing facility will be allowed to ensure the integrity of major computing assets. Except for essential personnel, visitors will be escorted at all times. Entry will be controlled by a badge reader.

Demonstration Area— No escort is required.

First Floor Meeting Room— No escort is required.

3.2.3 EDF Security Personnel

The EDF security staff consists of two receptionists who work staggered shifts from 7:00 AM until 6:00 PM.

3.3 Building Physical Security

3.3.1 General

The building physical security consists of electronic monitoring with alarming locally and remotely for fire and at an alarm central monitoring at Hechinger Headquarters on Pennsy Drive who would dispatch special police or call municipal police or emergency response teams. The entry-ways and outside parking lot are monitored on a 24-hour basis by camera observation.

3.3.2 Entry Control

Entry control is by key card during odd hours and by badge recognition during business hours. Certain accesses such as the loading dock and storage closets are secured with limited access key lock entry systems. The Telephone Switch Room, Telecommunications Rack, and Telephone Voice/Data Room are controlled by cipher lock.

3.3.3 Guard Force Response

The building owner maintains remote monitoring via video cameras, motion sensor, fire, and smoke alarm systems that initiate security guard response from approximately three miles away. HAIS will rely on municipal police and emergency response teams for other emergencies.

3.4 Equipment Tracking and Inventory

The Facility Manager and the System Manager shall ensure that all property is entered and controlled by the Uniform Property System, HAIS Practice 9-3-13. Both the Facility Manager and the System Manager will perform periodic audits of the physical property control system and issue Property Management Reports. Adjustments will be made for actual usage and maintenance events in the evolving EDF environment.

4. Personnel Security

4.1 Personnel Screening

Hughes corporate personnel office screens new hires according to the level of sensitivity of the position descriptions. HAIS routinely verifies references, degrees received, possible criminal records, professional licenses or affiliations, conflicting political affiliations, and employment.

4.1.1 General

Appendix B contains rules and regulations of Human Resources Practice 3-0-32A which apply to all Hughes employees.

4.1.2 Background Checks

This is not a requirement for this project, however, routine screening as discussed in Section 4.1 above is used for new hires.

4.1.3 Need-to-Know

None of the data in the ECS will be classified for National Security purposes. The highest classification will be company private and ECS project sensitive. Accordingly, only personnel with the need to process or handle company private and ECS project sensitive information will be given access to such data on a need-to-know basis for the highest level of sensitivity in the data at that time. There will be separate file servers for each area of project administration and system development with features that require privileged access by password security under network control.

4.2 Security Education and Training

4.2.1 Security Awareness

The System Manager will perform the following duties in support of the security program in consonance with the Company Practice 11-1-11, Security Education and Training.

- Orientation of new employees, subcontractors, and visitors to the security practices employed on the ECS network as it applies to their specific tasks or functions
- Acquaint employees with the techniques and devices that will be employed to backup critical data and methods to retrieve such data when necessary
- Methods of implementing and safeguarding password protection for data access
- Internal audit to assure proper use of backup and password protection
- Practicing good facility security procedures

4.2.2 Special Training Needs

Hughes Technology Services Company (HTSC) will train its employees either in-house or at vendor sponsored sessions in the use of special purpose test equipment, computer systems, data storage devices, network systems, operating system, applications software, etc. The ECS Maintenance and Operations group will sponsor training related to the ECS product as it evolves in the EDF support environment.

4.3 Network Access Control

4.3.1 Permanent Access

The Company Practice 18-2-2 provides details of our approach to access control of information systems. There will be specific provisions for the ECS as it evolves into a product. In general, for the EDF support environment, each user is assigned a unique code (user-id) that relates his/her identity. User-ids are administered by authorized security administrators only. User-ids are promptly removed for severed employees/users. Electronic approval, at a minimum, requires user identification and authentication through a user-id and password combination which serves as a personal signature. Passwords are nontrivial, are not shared by others, must be changed periodically, and are kept as company private information. Passwords are immediately changed if compromised. System default passwords are immediately changed from vendors settings and never used again.

Automated access procedures (e.g., log–on scripts) are kept as privileged data and do not contain unprotected passwords. We employ access control measures via operating systems, applications, and security software to ensure proper user identification; masking or encryption of sensitive data; discouragement of hackers repeated trials for entry by timeouts and reports; computing sessions are locked or disabled after a specified period of inactivity; privilege levels (e.g., read/write, read-only, and no access); audit trails; etc.

4.3.2 Visitor Network Access

The Plant Protection Office will provide direction to HTSC's system administrator in regard to determining the duration and level of access to be provided to visitors subject to approval by the ECS Project Manager. Guest accounts will be granted for both on and off-site access to certain data sets.

4.4 Badging

Program badges are magnetically encoded to grant access to the ECS area of the building. Those personnel who are authorized to access the computer area will have uniquely encoded badges. Visitors will not have encoded badges since they will be escorted while on HAIS premises. Certain Government personnel will be given project badges that provide permanent access to the EDF.

4.5 Records and Audits

Records and audits obtained by HTSC and others will be kept in a configuration database by the Configuration Manager to ensure proper use of documentation and procedures in the EDF; proper insight for program management into the performance of the EDF; and trend analysis within the support environment. This data will collectively be used for security assessments and contingency plans. Contingency plans include adequate backup and offsite storage of data, software, and documentation. Contingency plans are tested annually or more frequently if changes in operating environments indicate special needs. Software audits, network audits, equipment audits, and facility audits will be performed on an annualized basis to appraise project assets, deficiencies, inventories, and capabilities that might need adjustments, tuning, or enhancements, e.g., reallocation of space, modular growth, or stocking of consumables.

This page intentionally left blank.

5. Information Security

5.1 Privacy Data

The EDF operations shall support Sensitivity/Criticality Level 1 which is assumed to apply to the EDF operations in accordance with the definitions of NHB 2410.9 Exhibit 4-2; therefore, we will ensure the implementation of the following major security requirements during the EDF build-out evolutions.

Access Protection—Physical, procedural, and/or technical protective measures shall be provided that allow physical and/or logical management of authorization and access to the system and processing resources.

Configuration Management—A configuration management process shall be developed and maintained that monitors changes to any security-related and sensitive software, hardware, or procedure for the system.

Back-up Copies of Software—At least two generations of backups shall be maintained with the oldest generation being stored at a secure off-site location.

Physical Access—Systems shall be physically protected to prevent unauthorized access, theft, or destruction. Physical key locks shall be used to secure containers with critical data and prevent unauthorized removal of equipment or resources.

Network Access—Passwords shall be required for access to or from any network at appropriate levels of restricted access. Use of software that provides error checking and some error correction capability will be required when performing file transfers using networks.

Contingency and Disaster Recovery Plans—Contingency plans for applications and disaster recovery plans for computer installations shall be developed to provide for minimal interruptions and reasonable continuity of services. These plans will be prepared in accordance with Section 308 of NHB 2410.9 and the applicable provisions of Hughes Standard 18-2-2. Contingency plans are tested annually or more frequently as dictated by changes in operating environments.

Administrative Data Backup and Contract Deliverable Document Backup—At least two generations of backups shall be maintained with the oldest generation being stored at a secure off-site location. These data backups are the primary responsibility of the Business Operations Group and including Finance, Configuration Management, and Data Management. The System Manager shall ensure the integrity of network server backups.

5.2 Marking

We will mark company private/project sensitive documents clearly and conspicuously (not typed) in accordance with Chapter 12 of NHB 1620.3C and Company Practice 11-2-24 for internally generated company documentation.

5.3 Safeguarding and Storage

The Company Practice 11-1-12 describes safeguarding and storage procedures applicable to the EDF as follows:

Designating supervisory and senior employee at each ADP facility responsible for security who will brief ADP personnel and users regarding their security responsibilities on an at least annual basis.

Establishment of procedures for the destruction of sensitive tapes and disks, sensitive cards, printouts, carbons, and other materials in accordance with approved local facility procedures and equipment.

Provide suitable protective storage facilities, vaults, data safes or cabinets for sensitive tapes, disks, application programs, and other media at each ADP facility.

Develop written emergency and recovery procedures and related training programs for each ADP facility to include: 1) manual intervention and power shutdown; 2) protection of equipment against water, smoke, and other elements; 3) protection of data; 4) operation of portable fire protection and safety devices; and 5) evacuation of personnel.

5.4 Identification, Reporting, and Investigating Security Incidents and Violations

Hughes Corporate Policy 11-3-21 and Chapter 20 of NHB 1620.3C establish and support a program for the conduct of investigations concerning security matters and incidents of fraud, other violations, misconduct, abuse, and loss of company and Government property and/or sensitive data. The EDF shall follow these guidelines.

5.5 Inspection Program

Hughes agrees, under the terms of the security agreement with NASA, that the Government representatives have the right to inspect, at reasonable intervals, the procedures, methods, and facilities utilized by the Company in complying with the requirements of NASA security policy delineated in Chapter 37 of NHB 1620.3C and other provisions of the ECS contract. Hughes Corporate Policy 11-1-10 sets forth the terms of compliance and self-inspection applicable to the EDF.

5.6 Security Issues in the Segment Development Environment

In the following subsections, we identify support issues affecting security requirements that are specific to ECS project administration and segment development activities at the ECS Development Facility. The focus will be on noteworthy implementation support issues such as specific network connectivity or independence, private/public databases, access controls, data encryption, data storage, data backup, contingency planning, personnel security, etc. There is a common plan for disaster recovery as discussed in Section 6.9.

5.6.1 Project Management

Project Management is charged with the responsibility of administering a multi-level, multi-access secure information environment with distributed assets. The EDF Performance Measurement System contains project management and finance functions, a link to GSFC, and a link to HAC-Net. The development environment shares these communications links to GSFC and HAC-Net utilizing a separate file server with private partitions for separate data storage volumes. All systems have on and off-site data backup.

5.6.2 SCDO

The EDF network security requirements for ECS project development involve confidentiality and integrity considerations. Data confidentiality applies to passwords, which will be implemented as part of the EDF. Protection against intentional data modification applies to user authentication and authorization data within UNIX, Mac and PC system administration of the EDF network. All project development data, software, and algorithms require protection against both intentional and unintentional modification.

5.6.3 Flight Operations Segment

Network access for FOS shall be guarded by restricted network access, use of private volumes, and restricted data base access. The data bases for real-time telemetry and command processing require restricted access and may only be modified by the Data Base Administrator. Secure communication links between the FOS and spacecraft and instrument developers should be available when data (e.g., data bases) are transferred.

Sensitive hardware components (e.g., data encrypters) will require physical security to all unauthorized personnel.

5.7 Subcontractor Security

All subcontractors execute the Visitors Questionnaire and Agreement and agree to comply with the Security Instructions for Non-employees which is provided in Appendix A. Subcontractors are treated as permanent visitors in Hughes facilities and are issued ECS project badges upon written request by an authorized management employee of a Company organization by completion of a Badge Request Form 8212. Unescorted entry is authorized for a period of one year, subject to renewal which is subject to compliance with ECS project or company rules. Project badges are not issued to vendors, maintenance service personnel, and suppliers that are also involved in sales (Hughes Practice 11-1-3).

Privileged data shared with subcontractors will be safeguarded in accordance with nondisclosure agreements forming a part of the applicable contracts with Hughes and the Government in consonance with the NASA Federal Acquisition Regulations.

6. AIS Security

6.1 General

Automated information system security is an important issue for the success of the EOSDIS Core System project. Rapid advancements in computer technology, the need for effective communications to a wide audience, and the sharing of information in an open systems environment complicate the process of safeguarding information resources. Hughes will employ NASA standards as well as company practices to ensure information system integrity applicable to technical and administrative data, documentation, hardware, software, networks, and procedures. The degree of protection is commensurate with the value of information assets and risk to the ECS Project's success factors regarding the quality and integrity of data resources.

6.2 System Security Manager

The EDF computing system is managed by the system manager who performs system operations in the entire EDF and maintains Hughes capital equipment (office automation and administration) with support from vendor maintenance. The system manager will also act as the Computer Security Officer (CSO) to ensure compliance to computer network security procedures by system users. The procurement organization will perform installation and maintenance of ECS Contractor furnished equipment which is operated by the system manager. The system manager will perform installation and maintenance of Government furnished equipment. Accountability for the evolving EDF configuration baselines will be maintained by the Configuration Manager.

6.3 AIS System Security

The initial security plan for the EDF is to utilize UNIX system administration tools, router address filtering, virus defenses, and routine backup security measures. As the ECS development proceeds, the EDF will adopt a subset of the security functionality provided to the ECS. The subset will include a functional equivalent to Distributed Computing Environment (DCE) authentication/authorization security services.

6.3.1 System Overview of the Development Environment

The floor plan of the EDF is being maintained under configuration control as the *EDF Computer Floor Layout,* document #811-TD-007-001. This environment consists of the workstations, desktop computers (PCs and MACs), the EOS file server, ccMail servers, the Business Operations servers, associated communications equipment, LANs, and printers that support our development environment. All of this COTS hardware and software is intended to support the infrastructure of the ECS Project.

The PCs and MACs come in two basic configurations, a general one for the large percentage of users and an enhanced version for lead personnel who have additional requirements. All platforms have the basic tools including Microsoft WORD, EXCEL, POWER POINT, ccMail, and a drawing tool to support every day work activities. In the future, an X-Windows interface tool and possibly a scheduling tool will be added to the basic set of tools. The enhanced PC platforms will use the SCO/UNIX operating system, instead of DOS, in addition to the other tools. While the PCs and MACs currently have 14” color monitors, all future platforms will have high resolution 17” color monitors. The basic operations concept is that virtually all design and development work will be done from the desktop computers. With the X-Windows interface, the user will have access to the appropriate workstations and/or servers for their design/development work.

Security services for the ECS Project will be developed and tested in the EDF in the early Ir1 time frame. Development and testing will be accomplished using the DCE development tool kit. The applications, including the security capabilities, will be loaded into the hardware prior to shipment to the DAAC sites. The work effort in the field will be minimized, and the security systems will be in place to protect the ECS systems. The following subsections identify the site configurations for Ir1 and Release A.

6.3.1.1 Ir1 ECS Development Facility

6.3.1.1.1 Ir1 EDF Science Processing Hardware CI

The server and platform to be used at the EDF to support the Science Software Integration and Test (SSI&T) will be an SGI Power Challenger (to be used as a server), two Central Processing Units (CPU), a second SGI Indigo Server, and a SUN SPARC 20/50 workstation.

The applications supporting the Science Processing Hardware CI (SPRHW)-EDF-1 (Science Processor), SGI Power Challenger are SNMP Agent, CASEVision, IRIX 6.0.1, Interactive Data Language (IDL), International Mathematical Statistics Libraries (IMSL), C, C++, F77, F90, Ada, Software (SW) Configuration Management (CM), DCE Dev kit, and Scheduler Agent.

The applications supporting the SPRHW-EDF-2 (Science Processor), SGI Indigo Server are SNMP Agent, CASEVision, IRIX 5.3, IDL, IMSL, C, C++, F77, F90, Ada, SW CM, and Scheduler Agent.

6.3.1.1.2 Ir1 EDF Algorithm Integration and Test Hardware CI

The applications supporting the Algorithm Integration and Test Hardware CI (AITHW)-EDF-1 SUN SPARC 20/50 workstation are SNMP Agent, CASEVision, Document Viewing, SPARCworks, Solaris 2.3, IDL, IMSL, C, C++, F77, F90, Ada, SW CM, Rep Generator, DCE Dev kit, and Sybase Server (Ir1 only).

All processors (EDF and DAAC sites) are configured with a Compact Disk Read-Only Memory (CDROM) and 2 Gigabytes (Gbyte) of local disk. The CDROM is used to load software directly onto each machine. Loading can be accomplished using the network; however, for Ir1, the existing Version 0 Ethernet network is being used. DCE/Kerberos is a standard project requirement and is a part of the operating system. All systems are automatically ordered with an operating system and DCE.

Associated peripherals for the EDF include two RAID configuration (30 and 5 Gbyte), media readers for 8-mm tape, an 8-mm tape stacker, a CDROM, and a network connection to two Light Amplification by Stimulated Emission of Radiation (LASER) printers.

The planned ingest/interface testing platforms and attached peripherals are two SGI Power Challenge Ls, two CPUs, each with a 5-Gbyte RAID disk and one media reader, an 8-mm stacker tape drive, and a network connection to two LASER printers.

The MSS workstations will include a SUN SPARC 20/50 and an MSS server HP 755. The HP server will have a 5-Gbyte disk attached for data storage. The CSS will be an HP 755 with a 5-Gbyte RAID disk.

6.3.1.1.3 Ir1 EDF MSS

The applications supporting the MSS-EDF-1 (MSS Server) with 256 Megabyte (Mbyte) of storage are SNMP Agent, OpenView, HP UX 9.0.5, SW CM, and Rep Generator for Ir1 production. Additional support equipment includes an HP LaserJet 4M+, 12 ppm/14-Mbyte Random Access Memory (RAM) printer.

6.3.1.1.4 Ir1 EDF CSS

The applications supporting the CSS-EDF-1 (MSS Server) HP 755 with 256 Mbyte of storage and an HP 5-Gbyte disk storage are SNMP Agent, DCE Name, Security, HP UX 9.0.5, and SW CM.

The CSS-EDF-2 Bulletin Board (BB) Server will consist of a SUN SPARC 20/50, a CDROM, and a 96-Mbyte local disk. This equipment is supported by SNMP Agent, SW CM, Solaris 2.3, SPARCworks, C, C++, F77, and F90.

6.3.1.1.5 Ir1 EDF ISS

The ISS is supported by an Ethernet Hub.

6.3.1.1.6 Ir1 EDF Data Repository Hardware CI

The applications supporting the Data Repository Hardware CI (DRPHW)-EDF-1 [File Service Management System (FSMS) Server], SGI Power Challenger XL, two CPUs, 256 Mbyte, with a 30-Gbyte local disk are SNMP Agent, Network File System (NFS), IRIX 5.3, Sybase, and, C++.

The applications supporting the DRPHW-EDF-2 [Database Management System (DBMS) Server], SGI Power Challenger XL, two CPUs, 256 Mbyte, 4-mm media, with a 30-Gbyte local disk are SNMP Agent, NFS, IRIX 5.3, Archival Management and Storage System (AMASS) License [150 Terabytes (Tbyte)], and C++.

The applications supporting the DRPHW-EDF-4 (Robotics Archive) are EMASS G-series plus 3490 media with attached Network Transport Protocol (NTP) media (50) and 3490 media (50).

Additionally, the DRPHW will have two linear IBM NTP-type magnetic drives.

6.3.1.1.7 Ir1 EDF Ingest Client Hardware CI

The applications supporting the Ingest Client Hardware CI (ICLHW)-EDF-1 (Ingest Server), SGI Indigo Server with an SGI 6-Gbyte disk are SNMP Agent, Builder Xcessory, IRIX 5.3, and SW CM.

6.3.1.2 Release A ECS Development Facility

In Releases A, the Ir1 configuration will baseline the EDF for future ECS activity. The following equipment will be added to support Release A configuration. and development activities.

6.3.1.2.1 Release A EDF AITHW

The AITHW SUN SPARC 20/50 Workstation will be reconfigured to become the Planning Hardware CI (PLNHW), DBMS Server.

6.3.1.2.2 Release A EDF SPRHW

The server and platform to be used in Release A to support the SPRHW will consist of an SGI Power Challenger XL (to be used as a Science Processor), two CPUs, 8-mm media, a CDROM, and a Queuing Management Workstation, a SUN SPARC 20/71.

The SPRHW Queuing Management Workstation, SUN SPARC 20/50 is supported by the SNMP application, SW CM, and the Controlling Scheduling Software. (The DAAC site will have a local scheduler for operational activities).

6.3.1.2.3 Release A EDF ISS

The Release A ISS will be upgraded as follows:

a. ISS-EDF-1 will be a Fiber Distributed Data Interface (FDDI) switch, Atlantic Power Hub.

b. ISS-EDF-2 and -3 will be two FDDI concentrators, Synoptic Sys 2000.

c. ISS-EDF-4 will be 40 FDDI cables, Standard.

d. ISS-EDF-5 through -8 will be 4 Ethernet Hubs, Synoptic Sys 2000.

e. ISS-EDF-9 will be 10 FDDI cables, Standard.

6.3.1.2.4 Release A EDF MSS

The applications supporting the MSS-EDF-4 (MSS Server) with a 256-Mbyte hard drive are SNMP Agent, OpenView, HP UX 9.0.5, SW CM, Server SW, and Rep Generator. Additional support equipment includes an HP LaserJet 4M+, 12 ppm/14-Mbyte RAM printer. Additional capabilities associated with the server are two HP 5-Gbyte disk storage units.

The MSS-EDF-3 Workstation will include a SUN SPARC 20/71 SNMP Agent, Solaris 2.4, SW CM, Server SW, and Rep Generator.

6.3.1.2.5 Release A EDF CSS

The applications supporting the CSS-EDF-3 (MSS Server) HP 755 with 256 Mbyte of storage and an HP 5-Gbyte disk storage are SNMP Agent , DCE Name, Security, HP UX 9.0.5, and SW CM.

6.3.1.2.6 Release A EDF Test Center

The Test Center (TC) applications supporting the TC-EDF-1 Acceptance Unit Test (AUT) Server, SUN SPARC 1000E with 1 Gbyte and a 4-Gbyte disk using 8-mm, high-density tape are SNMP Agent, SW CM, Solaris 2.4, Motif, and Sybase.

Five additional AUT SUN SPARC 20/71 Workstations with 512 Mbyte of memory are supported by SNMP Agent, SW CM, Solaris 2.4, Motif, and Sybase.

6.3.1.2.7 Release A EDF Working Storage Hardware CI

The two Working Storage Hardware CI (WKSHW)-EDF-1/2 SGI RAIDs, 40 Gbyte each, do not require applications; but they are attached to and support the DBMS and FSMS servers.

6.3.1.2.8 Release A EDF DRPHW

The DRPHW-EDF-3 Operations Workstations/Document Server will consist of a SUN SPARC 20/71, 5 Gbyte, 128-Mbyte RAM, and will be supported by the SNMP Agent and SW CM.

The DRPHW-EDF-5 Operations Workstations/Document Server will consist of a SUN SPARC 20/71, 5 Gbyte, 128-Mbyte RAM, and will be supported by the SNMP Agent and SW CM.

Additionally, the DRPHW-EDF-3 and -5 jointly share or use 40 Gbyte of storage, an 8-mm tape stacker, and 8-mm tape.

6.3.1.2.9 Release A EDF ICLHW

The applications supporting the ICLHW-EDF-2 Ingest Backup Workstation, SGI Indigo with 4 Gbyte of storage are SNMP Agent, SW CM, and IRIX 5.3.

6.3.1.2.10 Release A EDF PLNHW

The PLNHW-EDF-1 DBMS Server will consist of a SUN SPARC 20/71, 5 Gbyte, 128-Mbyte RAM, and will be supported by the SNMP Agent, Sybase Scheduler, and SW CM.

The PLNHW-EDF-2 Planning Workstation will consist of a SUN SPARC 20/71, 5 Gbyte, 128-Mbyte RAM, and will be supported by the SNMP Agent, Class Capture, and Scheduling Agent.

6.3.1.2.11 Release A EDF Algorithm Quality Assurance Hardware CI

The Algorithm Quality Assurance Hardware CI (AQAHW)-EDF-1 Quality Assurance workstations consist of a SUN SPARC 20/71, that will be supported by the SNMP Agent and SW CM.

6.3.1.2.12 Release A EDF Data Management Server Hardware CI

The applications supporting the Data Management Server Hardware CI (DMGHW)-EDF-1 (DBMS Server) with a 128-Mbyte hard drive and a 6-Gbyte disk are SNMP Agent, Sybase, HP UX 9.0.5, C, C++, and Web Server Software. This equipment will be part of the development environment.

The applications supporting the DMGHW-EDF-2 (DBMS Server) with a 128-Mbyte hard drive and a 6-Gbyte disk are SNMP Agent, Sybase, HP UX 9.0.5, C, C++, and Web Server Software. This equipment will be part of the development environment.

The DMGHW-EDF-3 Operations Workstation will consist of a SUN SPARC 20/71, SNMP Agent, Solaris 2.4, Motif, Sybase Client Libraries, SW CM, and Server SW.

This equipment may be upgraded to an HP 755 machine.

6.3.1.2.13 Release A EDF FOS EOC

The applications supporting the MSS-EDF-5 (MSS Server) HP 755 with a 256-Mbyte hard drive are SNMP Agent, OpenView, HP UX 9.0.5, and SW CM. Additional support equipment includes two HP 5-Gbyte disk storage units shared with the CSS-EDF-4 Workstation.

The CSS-EDF-4 Workstation will consist of an HP 755 with a 256-Mbyte hard drive, and will be supported by SNMP Agent, Server Software, HP UX 9.0.5, and SW CM. Additional support equipment includes two HP 5-Gbyte disk storage units shared with the MSS-EDF-5 (MSS Server).

The MSS-EDF-6 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, Server SW, and Rep Generator.

The MSS-EDF-7 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, Server SW, and Rep Generator.

The MSS-EDF-8 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, Server SW, and Rep Generator.

6.3.1.2.14 Release A EDF FOS EOC

The applications supporting the EOC-EDF-1 Digital Equipment Corporation (DEC) Alpha 1000, 4/200, 6-Gbyte Dual Network (Real-Time Server) are SNMP Agent, SW CM, DEC FUSE, TK, C, C++, Rogue Wave, Sybase, OSF/1, and Power Builder.

The applications supporting the EOC-EDF-2 DEC Alpha 1000, 4/200, 6-Gbyte Dual Network (Real-Time Server) are SNMP Agent, SW CM, DEC FUSE, TK, C, C++, Rogue Wave, Sybase, OSF/1, and Power Builder.

The applications supporting the EOC-EDF-3 DEC Alpha 1000, 4/200, 6-Gbyte Dual Network (Real-Time Server) are SNMP Agent, SW CM, DEC FUSE, TK, C, C++, Rogue Wave, Sybase, OSF/1, and Power Builder.

The applications supporting the EOC-EDF-4 DEC Alpha 1000, 4/200, 6-Gbyte Dual Network (Real-Time Server) are SNMP Agent, SW CM, DEC FUSE, TK, C, C++, Rogue Wave, Sybase, OSF/1, and Power Builder.

The EOC-EDF-1 through 4 will be housed in two server racks.

The EOC-EDF-7 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, and SPARCworks.

The EOC-EDF-8 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, and SPARCworks.

The EOC-EDF-9 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, C, C++, and SPARCworks.

The EOC-EDF-10 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, C, C++, and SPARCworks.

The EOC-EDF-11 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, and SPARCworks.

The EOC-EDF-12 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, and SPARCworks. EDF-12 is supported by a 12-inch monitor.

The EOC-EDF-13 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, C, C++, and SPARCworks.

The EOC-EDF-14 Workstation will consist of a SUN SPARC 20/71, and will be supported by SNMP Agent, Solaris 2.4, SW CM, IDL, C, C++, and SPARCworks.

The EOC-EDF-15 HP LaserJet 4M+, 12 ppm/12-Mbyte RAM Printer.

The EOC-EDF-16 HP Laser Jet 4M+, 12 ppm/12-Mbyte RAM Printer.

The applications supporting the EOC-EDF-17 DEC Alpha 1000 200, 6-Gbyte Dual Network (File Server) are SNMP Agent and OSF/1 supported by a network attached RAID.

6.3.2 System Security

HAC Policy 18-2-2, Protection of Information Systems, will be administered for the security practices associated with password protection. UNIX system users will be issued passwords for access to EDF networked machines. Passwords will require changing on a periodic basis.

Accesses are provided on a machine-by-machine basis: a user cannot access all machines in the EDF unless they have the appropriate accounts. A system administrator, with super-user privileges, will administer user registration and access. PC/MAC password protection will be administered utilizing similar mechanisms to the UNIX environment.

The *EDF Network Configuration* (document 811-TD-006-001) and *EDF Routing Topology* (document # 811TD-005-003) show the EDF network security configuration hardware. These diagrams have been rendered at the gross level of network servers, hubs, and routers. Additional security measures apply at individual workstations as explained below.

Three levels of file access protection will be provided to UNIX-based files developed and located within the domain of the EDF network: user, group, and global. Access privileges at these levels include read-write, read-only, and no access. PC/MAC file access will be administered utilizing similar mechanisms to the UNIX environment.

Router address filters will be utilized to protect the EDF from intrusion from outside networks. The routers will be configured to filter traffic into and out of the EDF based on the Internet protocol (IP) address space identifier. Network packets with 'incorrect' addressing will be rejected by the router 'firewall'.

Defenses against known viruses will be employed where practical. Individual PCs and MACs will be equipped with the latest version releases of anti-viral software to alert EDF users of potential virus intrusions. UNIX system administrator tools will be analyzed and virus defenses employed, for the UNIX development environment.

Hughes Practice 11-1-12, Electronic Data Processing Security Program, and Hughes Policy 11-4-1, Emergency/Disaster Preparedness Program, will be followed for software backup procedures to help ensure against the loss of critical program data, software and algorithms. Program files will be periodically backed-up for maximum protection against long-term loss of valued data. The backup files are time-tagged to ensure minimal disruption for replacement of files, if required.

In later stages of the EDF life-cycle, similar security mechanisms will be employed as that employed with the ECS networks. At present, the HAIS plan is to utilize Distributed Computing Environment (DCE) authentication and authorization services for the protection of valuable ECS resources. This security environment is designed for distributed processing, offering a high degree of security assurance not found for distributed systems with conventional security practices. All user and process interactions are first authenticated to ensure the source (client) is who they say they are; then authorized, to ensure the correct use by the client of system resources. In this way, potential violators penetrating the router security firewall will fail authentication and will not be allowed access to system resources.

6.3.2.1 Hardware Security

The following protective measures apply to EDF automated information system hardware:

a. Physical Access Controls—Appropriate physical protections in the area where processing on the system takes place (e.g., locks on terminals, physical barriers around the processing area, etc.) These types of issues were detailed in Section 3.

b. Production, I/O Controls—HAIS will institute controls to ensure the proper handling, processing, storage, and disposal input and output data and media as well as access controls (such as labeling and distribution procedures) on the data and media.

c. Contingency Planning—Workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. They shall be coordinated with backup and recovery plans of any installations and networks used by the applications. System contingency plans will be implemented and tested regularly to assure the continuity of support in the event of system failure. These plans shall be known to users and coordinated with their plans.

d. Audit and Variance Detection—HAIS will implement controls which allow management to conduct an independent review of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures.

e. Hardware Maintenance Controls—HAIS has a system of controls used to monitor the installation of updates of hardware to ensure that the functions expected are performed and that an historical record of all changes is maintained. These controls include management approval of configuration changes and documentation of authorized changes.

f. Documentation—Controls in the form of descriptions of hardware, operations, and maintenance policy, standards, and procedures related to computer security to include backup and contingency activities are documented for AIS support staff as well as users.

g. Configuration Management Controls—These controls provide for the management process to review and determine changes to any security-related and sensitive hardware, software, or related policy, standards, and procedures.

h. Environmental Controls—These controls are designed to maintain a proper operational environment for personnel, hardware, software, and data storage. Environmental controls include but are not limited to temperature, humidity, ventilation controls, uninterruptible power, fire suppression, lighting, and water.

g. Incident Detection and Reporting—Procedural controls will be used to ensure the timely detection and reporting of significant computer security incidents, for determining the type of information in the report, and for appropriate problem resolution.

h. Storage Media Controls—Proper labeling, handling, and storage of data media with be provided at both on and off-site data storage facilities.

i. Trouble Desk—The System Manager will maintain a trouble desk to provide timely technical assistance and emergency response to problems as they arise.

j. Tracking and Inventory—The System Manager shall ensure that all property is entered and controlled by the Uniform Property System, HAIS Practice 9-3-13. The System Manager will perform periodic audits of the equipment control system and issue Property Management Reports. Adjustments will be made for actual usage and maintenance events in the evolving EDF environment.

6.3.2.1.1 Functional Components

Appropriate functional security requirements will be specified for the application and shall identify protective measures for the integration into hardware, software, and telecommunications resources.

6.3.2.1.2 Communications Controls

We have instituted protective measures that are designed to provide automatic encryption of certain private data types and passwords. Additionally, there is a formal procedure for the approval of communications links and to identify other network nodes that are permitted to access the AIS node.

6.3.2.2 Software Security

The following protective measures apply to EDF automated information system software:

a. Physical Access Controls—Appropriate physical protections in the area where processing on the system takes place (e.g., locks on terminals, physical barriers around the processing area, etc.) These types of issues were discussed in Section 3.

b. Production, I/O Controls—HAIS will institute controls to ensure the proper handling, processing, storage, and disposal of input and output data and media as well as access controls (such as labeling and distribution procedures) on the data and media.

c. Contingency Planning—Workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. They shall be coordinated with backup and recovery plans of any installations and networks used by the applications. System contingency plans will be implemented and tested regularly to assure the continuity of support in the event of system failure. These plans shall be known to users and coordinated with their plans.

d. Audit and Variance Detection—HAIS will implement controls which allow management to conduct an independent review of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such things as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles.

e. Software Maintenance Controls—Controls will be used to monitor the installation of and updates to application software to ensure that the software functions as expected and that a historical record is maintained of application system changes. Such controls will also help to ensure that only authorized software is allowed on the system. These controls include software configuration policy that grants managerial approval to modifications, then documents changes. HAIS will also include protection and monitoring software such as "virus" protection, configuration audits, authentication/authorization, password control, etc.

f. Documentation—Controls in the form of descriptions of hardware, operations , and maintenance policy, standards, and procedures related to computer security to include backup and contingency activities are documented for AIS support staff as well as users. Documentation will be coordinated with the AIS managers to ensure adequate application and installation documentation is maintained to provide continuity of operations.

g. Configuration Management Controls—These controls provide for the management process to review and determine changes to any security-related and sensitive hardware, software, or related policy, standards, and procedures.

h. Environmental Controls—These controls are designed to maintain a proper operational environment for personnel, hardware, software, and data storage. Environmental controls include but are not limited to temperature, humidity, ventilation controls, uninterruptible power, fire suppression, lighting, and water.

i. Incident Detection and Reporting—Procedural controls will be used to ensure the timely detection and reporting of significant computer security incidents, for determining the type of information in the report, and for appropriate problem resolution.

j. Network Access Controls—These controls provide protective measures such as network access passwords and error checking.

k. Logoff/Timeout Controls—Controls will be provided to automatically disconnect a terminal/client that has not been in communication with the CPU/server for a specific period of time.

l. Database Management System Controls—Controls will be provided to maintain integrity, availability, and confidentiality of all information resident in a database as well as provide access control and privileges.

m. Trouble Desk—The System Manager will maintain a trouble desk to provide timely technical assistance and emergency response to problems as they arise.

6.3.2.2.1 General Software Support

Software support will come from a variety of sources. The Procurement Organization will perform installation and checkout of Contractor furnished equipment, i.e., equipment purchased under contract funding, which is operated by the System Manager and operating systems. The System Manager will coordinate applications software support with assistance from vendors, consultants, and in-house experts. Developed software will be supported by the responsible engineer.

6.3.2.2.2 Audit Trails and Logs

The System Manager will collect audits and logs with the assistance of Quality Assurance as detailed in Section 6.7. Configuration management will baseline the audit trails and logs. Management will analyze the audit trails and logs for trends and anomalies pertaining to security issues.

6.4 Configuration Management

The EDF will have its own configuration Change Control Board (CCB). AIS Security will be a top priority for the CCB as it maintains documentation of baselined data, hardware, software, networks, and procedures. Records of property control and audits of inventory items, as well as AIS security records collected by the CSO, will be maintained. All data items shall be recorded in an automated data base system. Configuration Changes will be executed under the governance of the EDF CCB who will keep up-to-date records of AIS baseline status.

6.4.1 Configuration Change Controls

The objectives of configuration change control applicable to AIS security ensure that changes are completely defined and presented in a way that enables management to assess cost, schedule, and performance limits and impacts to the ECS Project. We will ensure that approved changes are instituted in an orderly and systematic manner with appropriate accountability to ECS Project management.

6.4.2 Security Evaluation of Configuration Changes

ECS management and the CSO will have the means and the record trail to evaluate AIS configuration changes both before implementation by the CCB process and after as the CSO performs regular audit and preventive maintenance (PM) of the AIS. The PM will witness trends in AIS usage, capacity, performance, and trouble reports. Contingency plans for validity in limiting the impact of possible natural disasters, other accidental losses or damages, or sabotage will be continually evaluated . The evaluations will include the adequacy of backup and offsite storage of data, software, and documentation.

6.4.3 AIS System Configuration Control

The CCB, under auspices of the EDF manager, controls documentation of baselined data, hardware, software, networks, and procedures. Change orders are implemented via CCB direction to the procurement organization or the system manager and as applicable to vendors, users, maintenance service personnel, etc. The EDF CCB will be subordinate to the Project CCB while implementing changes in support of requirements for the development segments. Details of this relationship to other project CCBs are contained in the Configuration Management Plan for the ECS Project, 101-102-MG1-001.

6.4.3.1 Baseline Control

The unique nature of the EDF as a contractor facility devoted to the development and support of the ECS requires some autonomy from the ECS Project for EDF operational concerns that affect its own unique baseline control. The EDF CCB will only have authority for some Class I and all Class II changes to the EDF, i.e., form, fit, function without impact to cost or schedule of the ECS Project. Class I changes, e.g., impacting EDF budget or those affecting the ECS product, will be escalated to the Project CCB. AIS security issues will be an integral part of the evolving EDF configuration baselining process.

6.4.3.2 Interim Support Instructions

The EDF CCB will initiate interim fixes to immediately resolve emergency problems as directed by the EDF manager. Such matters requiring emergency response could involve health and safety issues; disaster response; calls to emergency response teams (fire, police, etc.); matters requiring system emergency shut-down or maintenance; or exercise of approved contingency plans.

6.5 Operating Procedures

ECS Operations staff will provide accurate, up-to-date procedures, manuals, training, and emergency contacts. Documentation of maintenance and operational procedures are presently being established and will be accessible from a database format. This documentation includes exceptional procedures (such as power up and power down) and routine procedures (such as backups and reconfigurations). It is our intent to establish a reference volume with table of contents and index (by function and keyword) which will be available on-line and in hardcopy forms. All procedures will be tested in ad hoc as well as end-to-end testing scenarios with results kept and documented.

6.5.1 Startup, Shutdown, and System Failure Procedures

6.5.1.1 System Startup Procedures

The system startup procedures will include the following information to provide a sequential and accurate security checklist of each system's startup routine. This documentation will provide detailed information on each client configuration and network server.

Hardware and software configurations

User lists

Hardware and software revision levels

Step-by-step examples for boot and power up

6.5.1.2 System Shutdown Procedures

The system shutdown procedures will include the above information as well as the following addition.

Step-by-step description for shutdown and equipment power off

6.5.1.3 System Failure Procedures

It is critical to maintain complete, accurate, and current backups of all files and programs at the EDF as well as off-site to re-establish the ECS computing environment in the event of a disaster. Furthermore, HAIS also understands the additional need to protect against data loss caused by hardware/software errors and inadvertent deletions. The ECS maintenance and operations team is currently in the process of establishing procedures utilizing cmi (Hughes implementation of the Total Quality Management philosophy) techniques to ensure that these procedures are optimized for the evolving EDF environment.

In the event of a system failure, the following documentation, procedures, and equipment will be provided.

- System Failures
  - Minimum system bootup and operating procedures
  - Procedures for the manual initialization of operating systems and processes
  - Probable cause for failure troubleshooting guide
  - Isolation and repair procedures
- Network Failures
  - On-line network management software
  - Time Domain Reflectometers (TDRs)
  - Break out boxes
  - Power meters
  - Network Analyzers

On site and on-call maintenance will be utilized along with inherent design features of backup, redundancy and sparing to meet system availability objectives.

6.6 Individual Accountability

The operations personnel will ensure only authorized personnel are admitted to the computer room. Prior to any system being operational on the computer floor, an access control system will be set in place. Upon the receipt of an approved request for access to the computer floor from the EDF manager, this individual will have a personal badge encoded to provide access. Changes in access privileges will be closely monitored and will be documented monthly. The badge reader will keep a log of who entered the secure area. These reports will be continuously available to the ECS management.

Data integrity is an individual responsibility. The network personnel back up the system on a daily basis, but individuals must maintain individual workstations. Facilities will be provided to assist in regular backup of individual's work files utilizing both network and off-line storage.

6.7 System Stability

The ECS M&O Team's life-cycle methodology implements a flexible, structured approach to providing in-process reviews of all phases of hardware and software changes. This approach mitigates the risk of system outages or data loss by iterations of implementation phase reviews and formalized documentation of changes. Anticipated changes are matched against current system status recorded in the ECS change database and becomes part of the implementation process.

6.7.1 Monitoring

The ECS approach to effective system monitoring is based upon establishing a specific methodology. The key parameters of this methodology are defined for calibration. We then spend our efforts tuning goals, continuously monitoring performance, and concentrating effort on the factors most affecting system performance. Our solution is designed to ensure the following critical goals are met:

Maximum network availability;

Minimum interruption during service functions;

Emphasis on preventive maintenance;

Expedient response to corrective maintenance and service requests;

Single focal point for reporting malfunctions, requesting service, or video conference support; and

Trend analysis of all anomalies.

6.7.2 Control of Work Flow

The ECS M&O organization allows for a centralized point of contact to help balance the load across systems. It is M&O's goal to be proactive to ensure the efficient throughput on all systems at all times. Close coordination of the systems' communications network with an aggressive monitoring and reporting scheme will allow us to have a continuous current analysis of the system processing loads. Scheduling of special jobs will be coordinated through M&O management. The user will call and request special exemption of standard queuing from the M&O staff. The M&O staff will notify all users that the system may be slower or that they must logoff for a set period of time.

6.7.2.1 Automated Logs

The operations staff is required to perform a large number of monitoring and reporting functions. Although these tasks are critical, they are also time consuming. Therefore, one of the areas where we see a potential for low-cost innovation is the introduction of automated monitoring and reporting logs. These logs will automatically check the network, gather I/O and CPU load information, and detail the results in a written report. It is our intention to evaluate such networking products as HP Open View over the coming months as the network management system (NMS) for the EDF.

6.7.2.2 Manual Logs

Where possible, we will institute automatic, computer-based logging procedures. If manual logging needs to take place, operations personnel will be trained on the usage of standard logs and will maintain this information in a central place with all other logs.

6.8 Software Protection

The M&O Team will support a common archive for system software. This archive will provide the operations staff with software and a checklist of required procedures and frequency of use to ensure the best reliability. One objective is to have similar file systems across the distributed system to perform easy, fast maintenance and reduce the dependency on specific personnel. This objective will be achieved with a standardized directory tree structure based on common practices.

The maintenance of a file system can be enhanced by using a source code control system to maintain different versions of system configuration files and allow revisions to earlier versions when it is necessary.

6.8.1 Software Design and Development Activities

Security issues related to software design and development activities have been detailed in Section 5.6.

6.8.2 Master Copy

Master copies of installed software are maintained under lock and key at a central repository. Critical applications are also maintained at the off-site storage facility. Developed software is backed up daily on the networks. Backup tapes from the network are maintained off-site.

6.8.3 Software Modification Activities

As system software enhancements and successor products become available, we will provide a tradeoff analysis of benefits, drawbacks, and estimates of time to complete installations. Compliance with user and site license agreements are continuously monitored. Our goal is to provide the latest versions of the currently licensed and installed system software. This will include corrective code, updates, and enhancements to the system software. We will perform regression testing for impact or adverse reaction of interactive applications, utilities and operating systems to prevent problems within current and future software configuration baselines.

6.8.3.1 Software Standards and Quality Assurance

Software development and control procedures will be implemented by the operations task managers as prescribed by contractor practices and software control plans. The applicable software assurance standards and requirements will be those contained in Hughes Management Directive 19-60-00, Software Quality Assurance, and other command media related to the Hughes' quality activities (Table 6-1). Software acceptance, verification, and traceability

Table 6-1. Applicable Contractor Manuals and Procedures (1 of 2)

Discipline	Contents
Engineering	
Numerical Reliability Analysis	Establishes guidelines for minimum reliability analysis requirements and approved failure rates
Failure Mode and Effects Analysis	Establishes guidelines for conducting failure modes and effects analysis
Management Directives Manual 47 506 series 507 series	5-0-6 series defines software management practices; 5-0-7 defines management requirements for the attainment of safe systems and products
Product Assurance: hardware and software	
Hughes Manual 614 which includes:	
- Subcontractor requirements	Defines requirements that selectively apply to subcontractors
- Program quality requirements Both H/W and S/W	Designates applicable program quality requirements
- Failure reporting and corrective action	Describes requirements and responsibilities for reporting analysis, corrective action, closeout of problems, and failures occurring during test of equipment
Hughes Applied Information Systems, Inc. (HAIS) Instructions 5-0-0 5-0-1 Integration and Test (I&T) 5-0-2 Internal Reviews 5-0-6 Software Engineering	5-0-0 establishes general practice for systematic orderly management of engineering activities within HAIS 5-0-1 establishes I&T practices within HAIS. See Paragraph 10. 5-0-2 establishes requirement for performing internal reviews of HAIS products. 5-0-6 establishes software engineering practices for design, coding, test, and documentation of computer software and firmware for mission software.
Product Assurance, Software Management Directives Manual 47 Company Practices 19-60-00	Defines Company and HAIS software quality assurance requirements
HAIS Instructions 19-12-001 Statistical Process Control (SPC) Certification /Assurance 19-12-003 Program Quality Requirements 19-13-001 Work Instructions	• Provides initial/periodic verification that personnel/equipment meet approved standards when SPC is used in manufacturing • Includes instructions for preparation, coordination, & application of QA requirements • Provides instructions on the use of detailed h/w manufacturing guidelines

Table 6-1. Applicable Contractor Manuals and Procedures (2 of 2)

Discipline	Contents
19-14-001 Quality Records and Traceability Requirements	• Provides instructions on the use, control, and retention of quality records and traceability data
19-15-001 Corrective Action	• Gives instructions ensuring prompt, effective implementation of corrective action to deficient conditions
19-17-001 Quality Audits	• Provides instructions for conducting QA audits
19-17-001A Audit Levels	• Defines levels, coverage, and frequency of QA audits
19-21-004 Drawings, Documentation, and Changes	• Defines QA participation in CM/DM activities
HAIS Instructions	
19-22-001 Measurement and Test Equipment	• Defines the system for control and calibration of test equipment
19-31-001 Supplier Control System	• Provides instructions for the evaluation, approval, and monitoring of vendors
19-32-001 Procurement Controls	• Provides instructions for QA review of procurement documents
19-33-001 Work Transfer Controls	• Provides procedures for review of incoming/outgoing Work Authorization Documents
19-41-001 Receiving Inspection and Test	• Instruction for the receipt, processing, inspection, and test of incoming materiel
19-42-003 Work In-Process Inspection/Test	• Establishes quality controls for the manufacture of h/w
19-42-005 Test Support	• Provides instructions for QA support of test activities
19-42-101 Planner/Screener Certification	• Provides guidelines for the tailoring of planning/procurement controls
19-43-001 Final Inspection and Test	• Provides instruction for QA verification of final product test and inspection
19-44-001 Material Handling, Storage, and Delivery	• Provides instructions for the packaging, handling, and storage of material to ensure protection of product quality
19-45-001 Non-conforming Material Control	• Provides instructions for control and disposition of non-conforming material
19-47-001 Identification of Quality Status	• Establishes the control and use of QA stamps
19-52-001 Control of Government/Custom Property	• Guidelines for inspection and control of Government/customer property
19-60-001 Division Software Quality Assurance	• Establishes procedures and responsibilities for Division-level QA activities

requirements shall be those described in each software control plan. Configuration control requirements that ensure proper management of changes to software and its related technical documentation will also be imposed and audited by QA for conformance to media such as plans, practices, procedures, and program instructions.

6.8.3.2 Acceptance Testing

The M&O Team will provide reliable, tested software systems, including production operating systems, consistent with vendor release and maintenance, for all supported computer systems from supercomputers to desktop workstations. The HAIS approach will provide maximum availability while improving the system and maintaining supported versions of software. HAIS will also ensure the operational capability of all production software through system upgrades and hardware changes.

Validation of security features will be incorporated into development baselines as well as every regression testing scenario.

6.9 Disaster Recovery

The EDF manager shall prepare an Emergency Preparedness Plan (EPP) which shall address the Emergency Organization and Employee Instructions. The subsections below shall address procedures for minimizing damage in the event of a disaster and recovering from any emergency interruption in service. EDF operations utilizing this plan will be able to recover essential application and operating system files, protect personnel, computing equipment, and contact key personnel and vendors.

6.9.1 Major Facility Loss

Within the EDF facility, specific personnel are assigned to an Emergency Preparedness Organization (EPO). This team assists in the execution of the EPP and provide guidance to employees during an emergency. The team members will wear hard hats embossed with the green safety committee emblems during actual/practice drills. Each of the team members assignments will be assigned to two persons, a designate and an alternate. The assignments consist of the following:

Site Executive-In-Charge

EDF Manager

Emergency Preparedness Coordinator

Impairment/Restoration Coordinator

Building Coordinator

Facility Security Coordinator

Floor Coordinator

Area Monitor

Specialized Monitors

Exit Monitors

On-Duty Security

Holding Area Monitors

The team will execute an evacuation checklist. Detailed instructions are provided as part of employee orientation for evacuation, medical emergencies, natural disasters, fire safety response, snow emergency, etc.

6.9.2 AIS Hardware or Software Protection; Loss of

Employees will be made aware of the value of computing equipment, software, and data. They will be encouraged to protect it in an emergency. However, safety must be considered first and employees must not place themselves in jeopardy of serious injury at any time. Representative response scenarios are:

Environmental Hardware Malfunction

Air Conditioning Units—If an air conditioning unit malfunctions in the computer room , refer to the computer center emergency contact list. It is important for the individual who makes the call to remain as close as is safe to the problem area until physical plant personnel arrive. Follow maintenance procedures in the event of a necessary emergency shut-down.

Power Distribution Units—If these units fail, refer to the appropriate maintenance contact from the computer center emergency contact list.

Fire Emergency/Alarms

Notify the local fire department by dialing 911 and pull the fire alarm. Notify the EDF security staff. Personnel not involved with detection/recovery should start evacuation immediately according to the EDF's general evacuation procedure. DURING A LEVEL 1 ALERT ONLY — power-off nearby equipment if the fire is confined to a small area. If it is determined at any time that the computer system should be shut down, locate one of the EMERGENCY POWER SHUTDOWN switches at each exit and depress the button. Fire extinguishers are available for use in the Computer Center. Extinguishers from the office areas should not be used on computer equipment.

A water sprinkler system is in place and will be activated by heat. If there is no fire and a sprinkler is activated unnecessarily and/or ceiling water pipes begin to leak, plastic sheets or salvage covers should be used immediately to cover and protect computer equipment. Turn off power immediately, then use plastic sheets.

Disaster Recovery Storage and Backup Operation Plan and Schedule

The EDF stores all systems and applications programs, datasets, and files for full systems recovery. These files are stored daily on-site and weekly at an off-site location. A schedule and procedure for backups will be maintained by HTSC.

6.9.3 Destruction of System Files, Programs or Procedural Documentation

An electronic version of system files, programs, and procedural documentation is maintained on-site and off-site as previously discussed. In the event of a loss, this information will be recoverable from archives.

6.9.4 Review and Testing

Exact dates are set up at 30 days in advance for testing system recovery contingency plans. Three weeks prior to testing, duplicate sets of backups are run for the system to be tested. Tapes have a one month expiration date. One copy remains in the library. The other copy follows the off-site rotation procedure for recovery.

Necessary computer operators designated by supervision perform the test. Other operations personnel and Quality Assurance representatives observe. The test is run immediately after a complete set of backups are run. The tapes to be used are those that most recently returned from off-site storage for testing. A cold start is performed on the computer system using standard operating procedures. A comparison is made of the two sets of backups to verify the system is in good working order.

This page intentionally left blank.

7. Security Issues Requiring Coordination with NASA

No special issues need to be resolved at this time.

This page intentionally left blank.

8. Hughes Internal Policies

Hughes-Internal Security Policies (Informational)

The following documents address various information security topics for which the GSFC Security Office requested information. These selected Hughes Aircraft Company policies and practices are provided for information purposes:[1]

General

11-1-1, Security Objectives and Organization

11-1-2.1, Plant Protection Responsibilities - Controls and Procedures

11-1-3.1, Physical Security, HAIS, Building 402

11-1-3.2, Lock and Key Control System, HAIS, Building 402

11-1-5, Security Reports

11-1-9, Disciplinary Actions for Security Violations

11-1-10, Security Inspections

xx-xx-xx, Use of Computer Systems **(new draft)**

Protection of Property/Inventory Control

9-3-13**,** Uniform Property System

Computer Security Awareness Training

11-1-11, Security Education and Training

Incident Reporting

11-1-5, Security Reports

18-0-6, Audit Access to Program Documentation and Data

Software Backup Procedure

11-1-12, Electronic Data Processing Security Program

11-4-1, Emergency/Disaster Preparedness Program

Protection of Proprietary and Copyrighted Software

2-2-7, Reproduction of Copyrighted Material

[1] Note that some of these policies were written for a classified environment and require tailoring to suit civilian-agency needs.

xx-xx-xx, Licenses **(new draft)**

SE-1-001, Project Shareware/Freeware Policy

Control of User Computer Access

18-2-2, Protection of Information Systems **(new draft)**

SE-1-003, Procedures for Access to the ECS Web Server

Information Security

11-2-24, Company Private Information

Personnel Security

11-3-1, Security Approval of Eligibility for Employment

11-3-21, Security Investigations

11-3-22, Civil or Criminal Processes Directed Against an Employee

Disaster Recovery/Prevention

11-4-1, Emergency/Disaster Preparedness Program

11-4-9, Fire Prevention, Protection, Suppression and Life Safety Programs

11-4-10, Hazardous Processes

Appendix A
Badging Policy at the
ECS Development Facility

This section is not available in electronic copy.

This page intentionally left blank.

Appendix B
Human Resources Practice
3-0-32A
Employee Rules and Regulations

This section is not available in electronic copy.

This page intentionally left blank.

Abbreviations and Acronyms

ADP	automated data processing
AIS	automated information system
CCB	change control board
CDR	critical design review
COTR	contracting officer’s technical representative
COTS	commercial off-the-shelf
CSO	computer security officer
CSPP	computer security and privacy plan
DAAC	distributed active archive center
DADS	data archive and distribution system
DCE	distributed computing environment
DID	data item description
ECS	EOSDIS Core System
EDF	ECS Development Facility
EOSDIS	Earth Observing System Data and Information System
EP	Evaluation Package
EPO	Emergency Preparedness Organization
EPP	Emergency Preparedness Plan
GNMP	Government Network Management Profile
GSFC	Goddard Space Flight Center
HTSC	Hughes Technical Services Company
IP	Internet protocol
M&O	Maintenance and Operations
MSFC	Marshall Space Flight Center
NCSL	National Computer System Laboratory
NMS	network management system
NRP	National Resource Protection
PGS	Product Generation System

RDBMS	relational data base management system
RDE	Release Development Environment
SCDO	Science and Communications Development Office
SDR	system design review
SMDS	Switched Multi-megabit Data Service
STL	Science Technology Laboratory
TDR	Time Domain Reflectometer